FIG.1

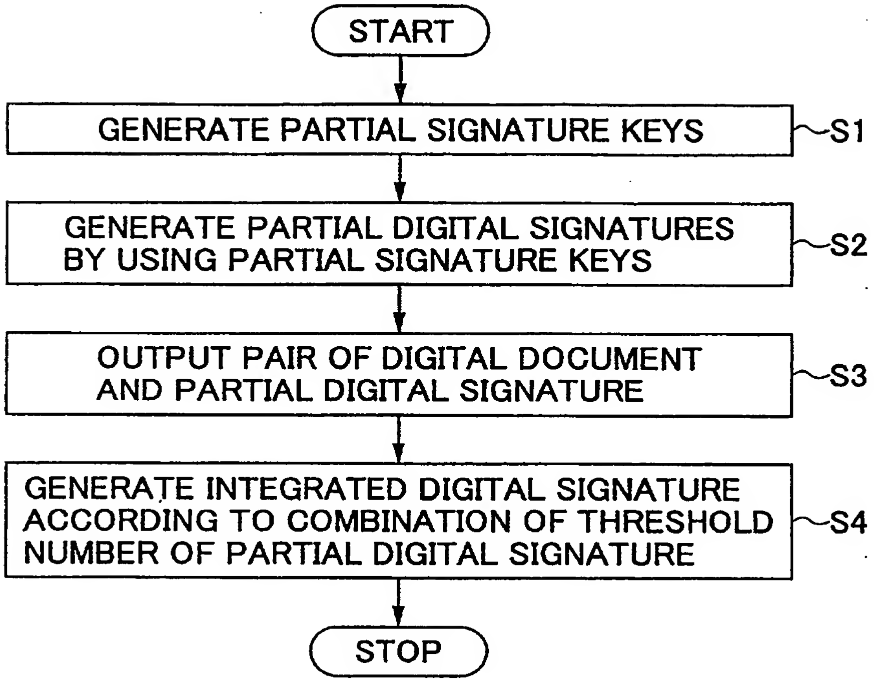

START
GENERATE PARTIAL SIGNATURE KEYS
S1
GENERATE PARTIAL DIGITAL SIGNATURES BY USING PARTIAL SIGNATURE KEYS
S2
OUTPUT PAIR OF DIGITAL DOCUMENT AND PARTIAL DIGITAL SIGNATURE
S3
GENERATE INTEGRATED DIGITAL SIGNATURE ACCORDING TO COMBINATION OF THRESHOLD NUMBER OF PARTIAL DIGITAL SIGNATURE
S4
STOP

FIG.2

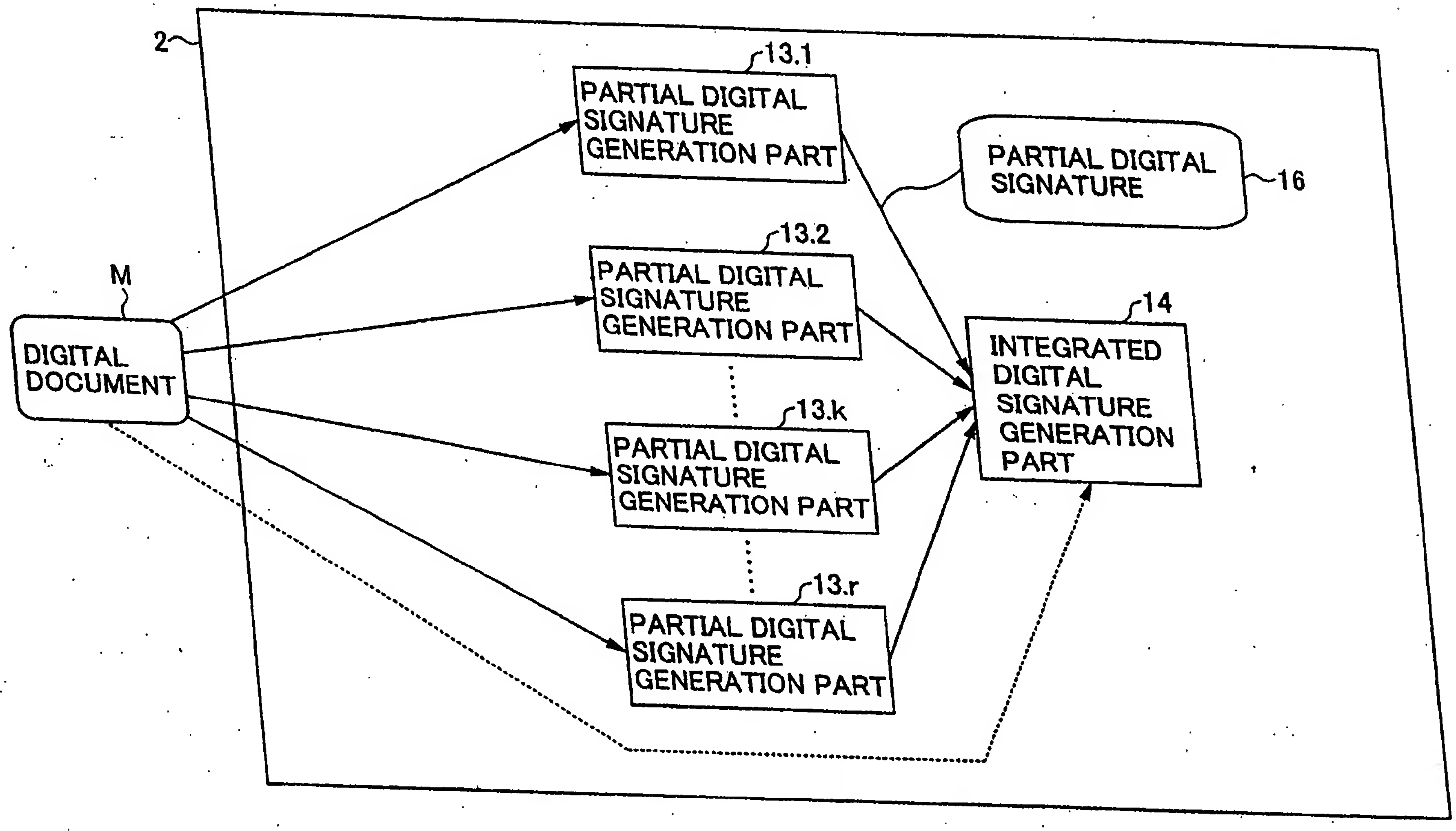

2
M
DIGITAL DOCUMENT
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PARTIAL DIGITAL SIGNATURE
16
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART

FIG.3

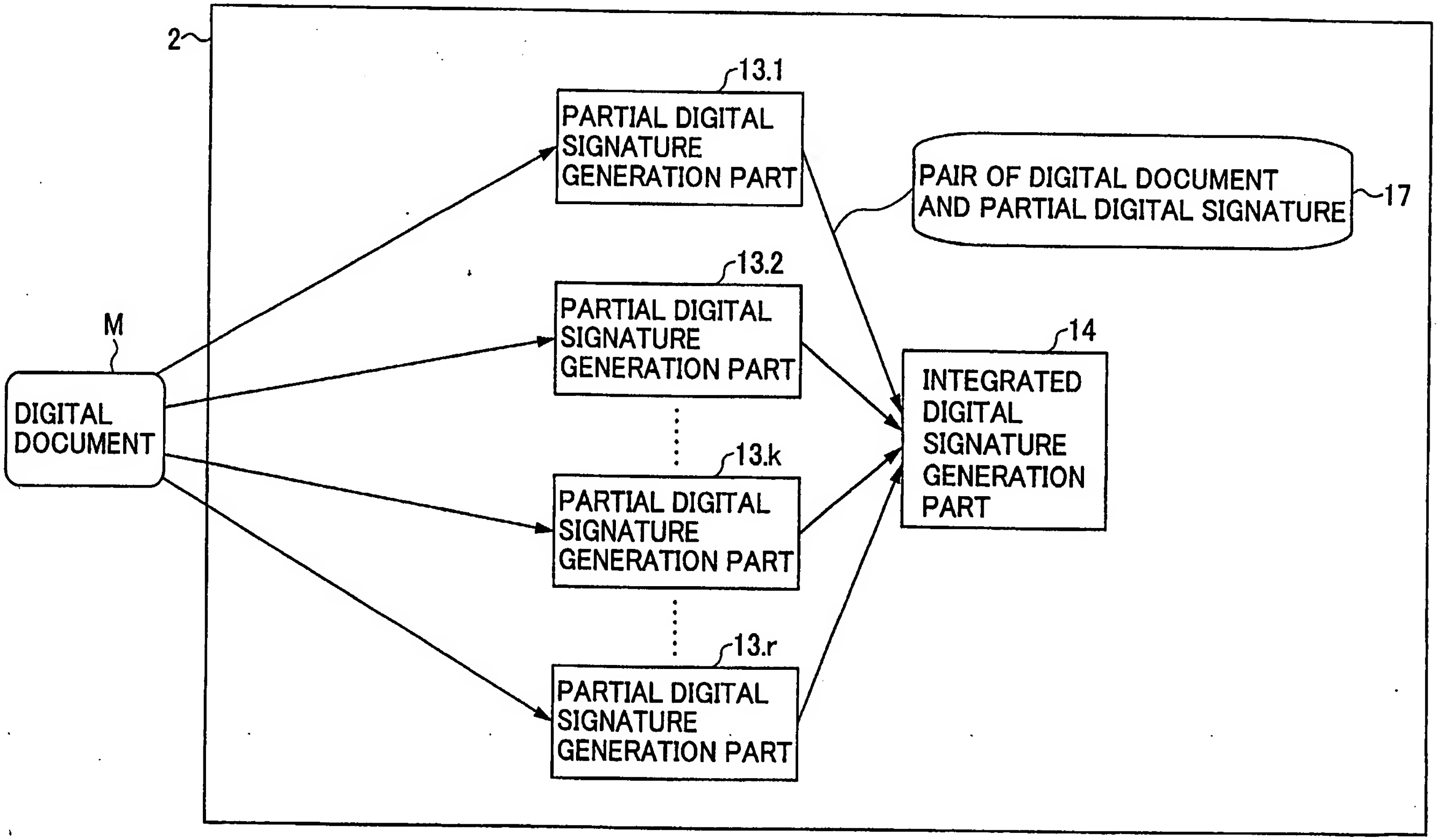

2
M
DIGITAL DOCUMENT
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PAIR OF DIGITAL DOCUMENT AND PARTIAL DIGITAL SIGNATURE
17
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART

FIG.4

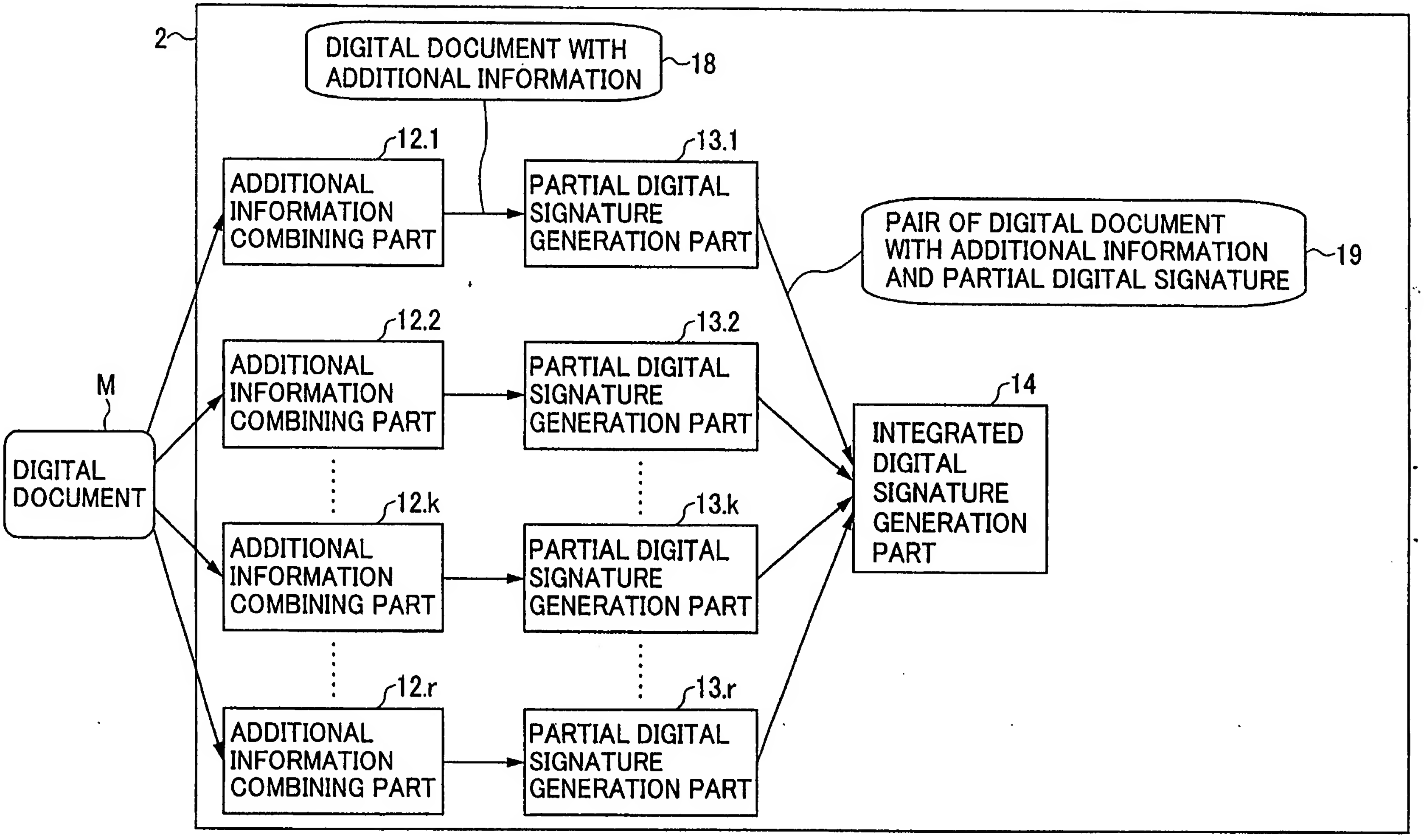
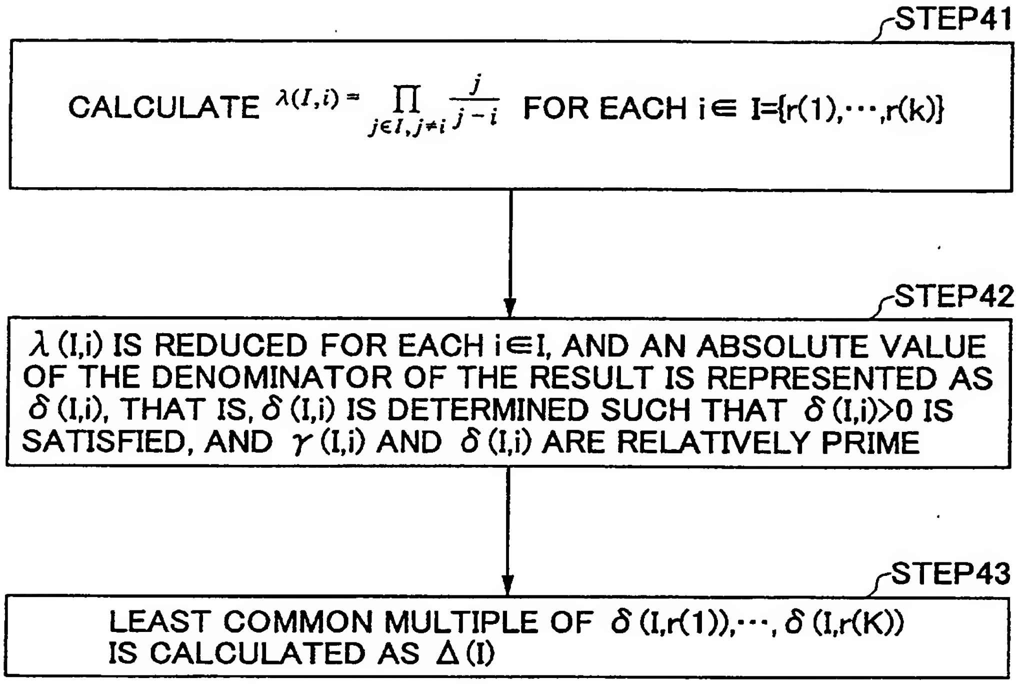

2
DIGITAL DOCUMENT WITH ADDITIONAL INFORMATION
18
M
DIGITAL DOCUMENT
12.1
ADDITIONAL INFORMATION COMBINING PART
12.2
ADDITIONAL INFORMATION COMBINING PART
12.k
ADDITIONAL INFORMATION COMBINING PART
12.r
ADDITIONAL INFORMATION COMBINING PART
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PAIR OF DIGITAL DOCUMENT WITH ADDITIONAL INFORMATION AND PARTIAL DIGITAL SIGNATURE
19
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART

FIG.5



CALCULATE $\lambda(I,i)=\prod_{j\in I,j\neq i}\frac{j}{j-i}$ FOR EACH $i\in I=\{r(1),\cdots,r(k)\}$

λ (I,i) IS REDUCED FOR EACH $i\in I$, AND AN ABSOLUTE VALUE OF THE DENOMINATOR OF THE RESULT IS REPRESENTED AS δ (I,i), THAT IS, δ (I,i) IS DETERMINED SUCH THAT δ (I,i)>0 IS SATISFIED, AND γ (I,i) AND δ (I,i) ARE RELATIVELY PRIME

LEAST COMMON MULTIPLE OF δ (I,r(1)),$\cdots$, δ (I,r(K)) IS CALCULATED AS Δ (I)

FIG.6

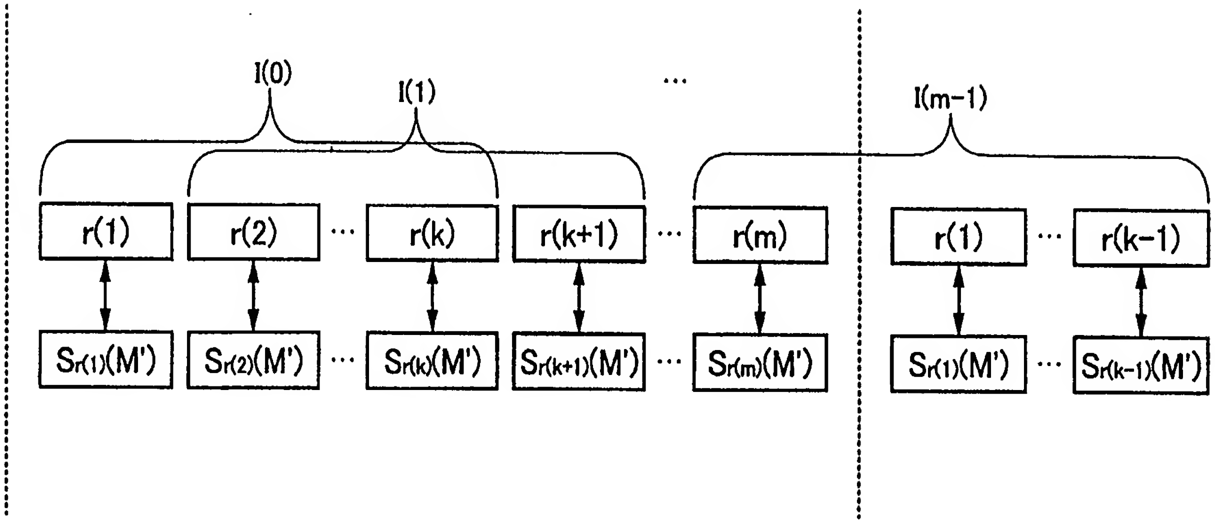

I(0)
I(1)
…
I(m−1)
r(1)
r(2)
r(k)
r(k+1)
r(m)
r(1)
r(k−1)
Sr(1)(M')
Sr(2)(M')
Sr(k)(M')
Sr(k+1)(M')
Sr(m)(M')
Sr(1)(M')
Sr(k−1)(M')

FIG.7

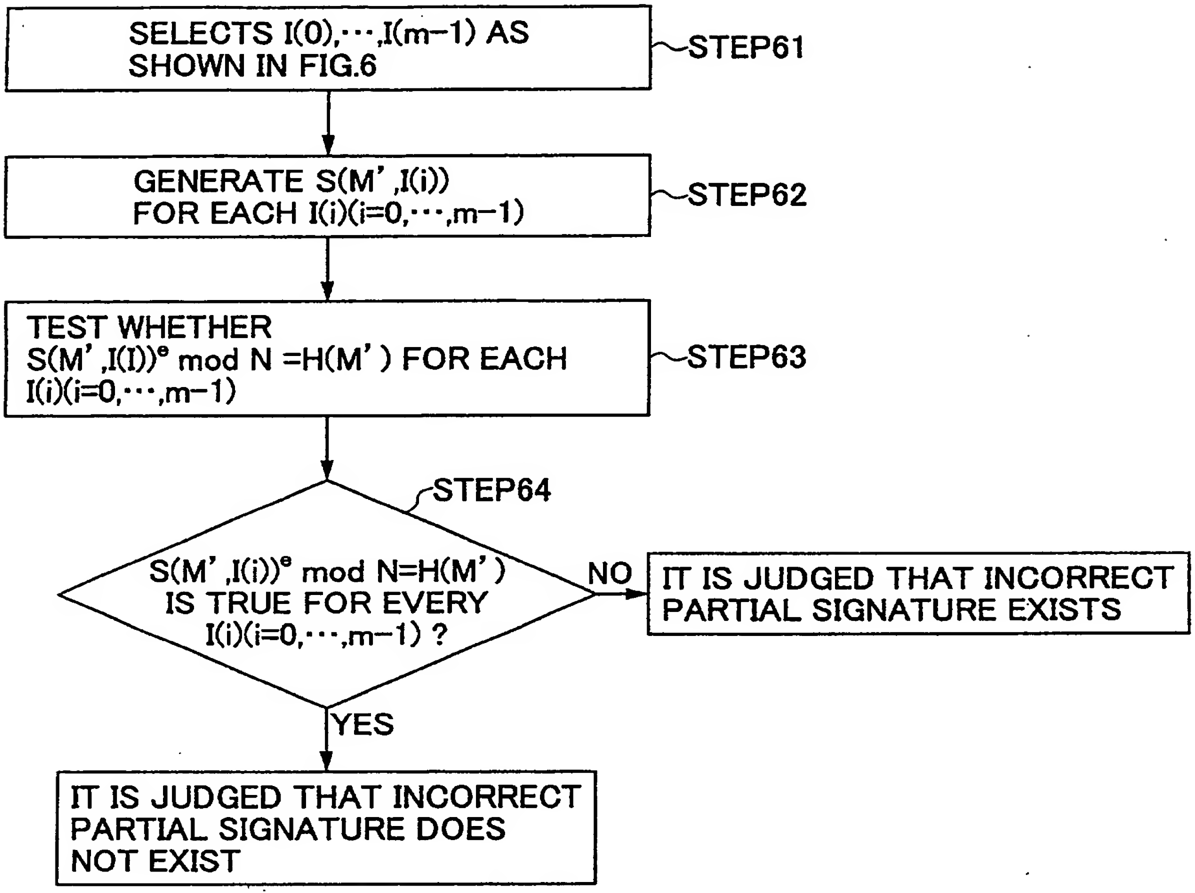

SELECTS I(0),···,I(m−1) AS SHOWN IN FIG.6
STEP61
GENERATE S(M',I(i)) FOR EACH I(i)(i=0,···,m−1)
STEP62
TEST WHETHER S(M',I(I))^e mod N =H(M') FOR EACH I(i)(i=0,···,m−1)
STEP63
STEP64
S(M',I(i))^e mod N=H(M') IS TRUE FOR EVERY I(i)(i=0,···,m−1) ?
NO
IT IS JUDGED THAT INCORRECT PARTIAL SIGNATURE EXISTS
YES
IT IS JUDGED THAT INCORRECT PARTIAL SIGNATURE DOES NOT EXIST

FIG.8

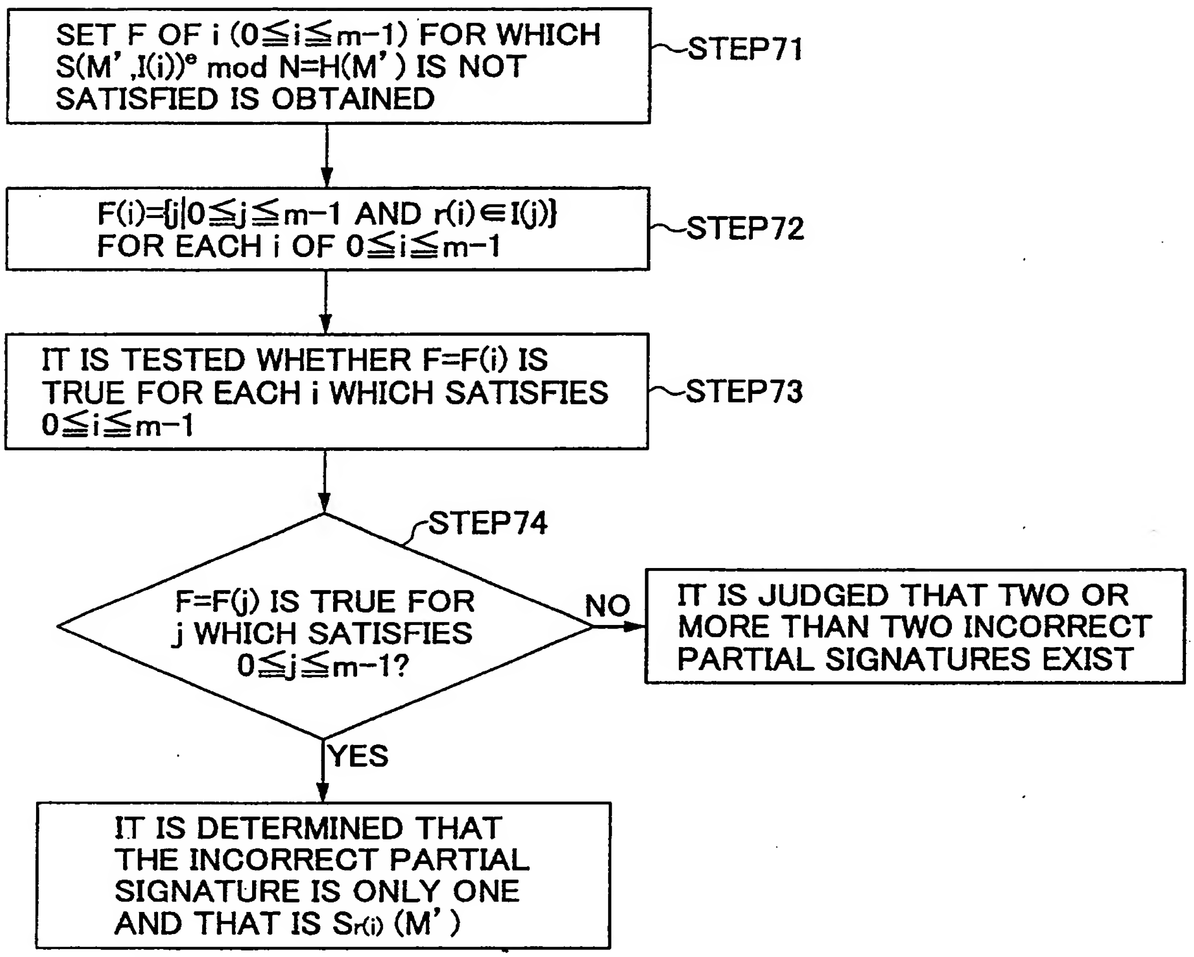

SET F OF i (0≦i≦m−1) FOR WHICH S(M',I(i))^e mod N=H(M') IS NOT SATISFIED IS OBTAINED
STEP71
F(i)={j|0≦j≦m−1 AND r(i)∈I(j)} FOR EACH i OF 0≦i≦m−1
STEP72
IT IS TESTED WHETHER F=F(i) IS TRUE FOR EACH i WHICH SATISFIES 0≦i≦m−1
STEP73
STEP74
F=F(j) IS TRUE FOR j WHICH SATISFIES 0≦j≦m−1?
NO
IT IS JUDGED THAT TWO OR MORE THAN TWO INCORRECT PARTIAL SIGNATURES EXIST
YES
IT IS DETERMINED THAT THE INCORRECT PARTIAL SIGNATURE IS ONLY ONE AND THAT IS S_r(i) (M')

FIG.9

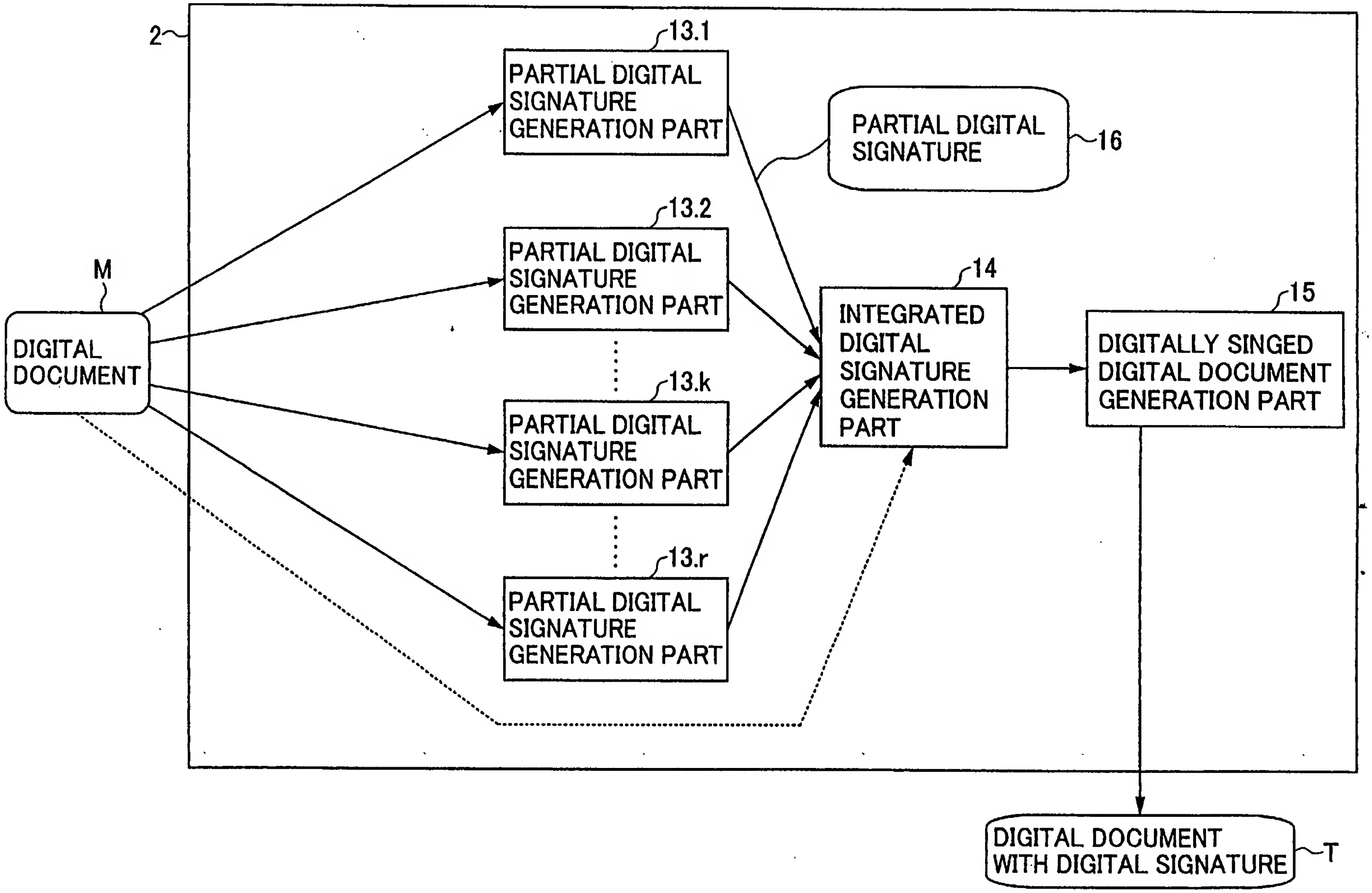

2
M
DIGITAL DOCUMENT
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PARTIAL DIGITAL SIGNATURE
16
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART
15
DIGITALLY SINGED DIGITAL DOCUMENT GENERATION PART
DIGITAL DOCUMENT WITH DIGITAL SIGNATURE
T

FIG.10

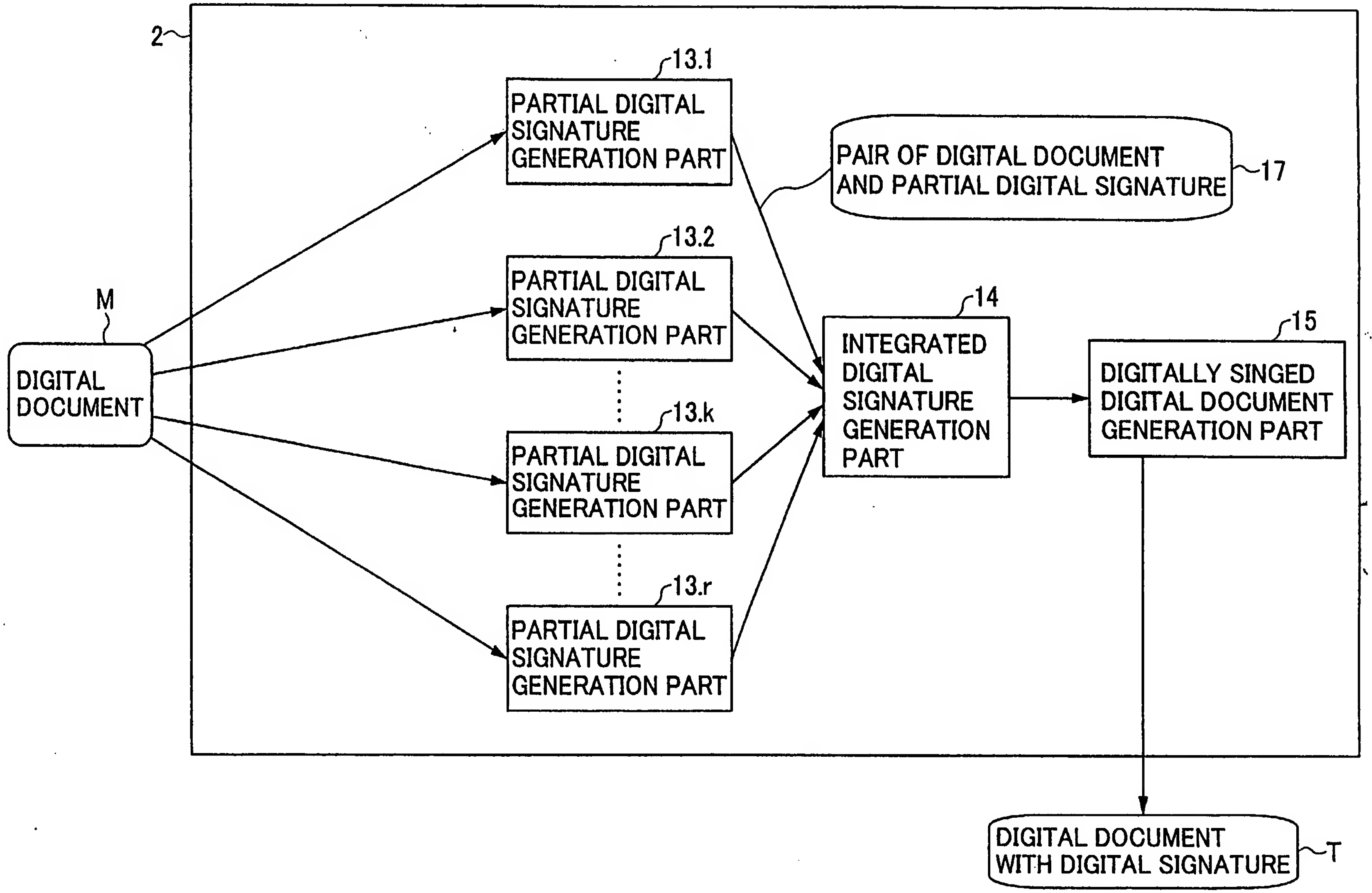

2
M
DIGITAL DOCUMENT
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PAIR OF DIGITAL DOCUMENT AND PARTIAL DIGITAL SIGNATURE
17
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART
15
DIGITALLY SINGED DIGITAL DOCUMENT GENERATION PART
DIGITAL DOCUMENT WITH DIGITAL SIGNATURE
T

FIG.11

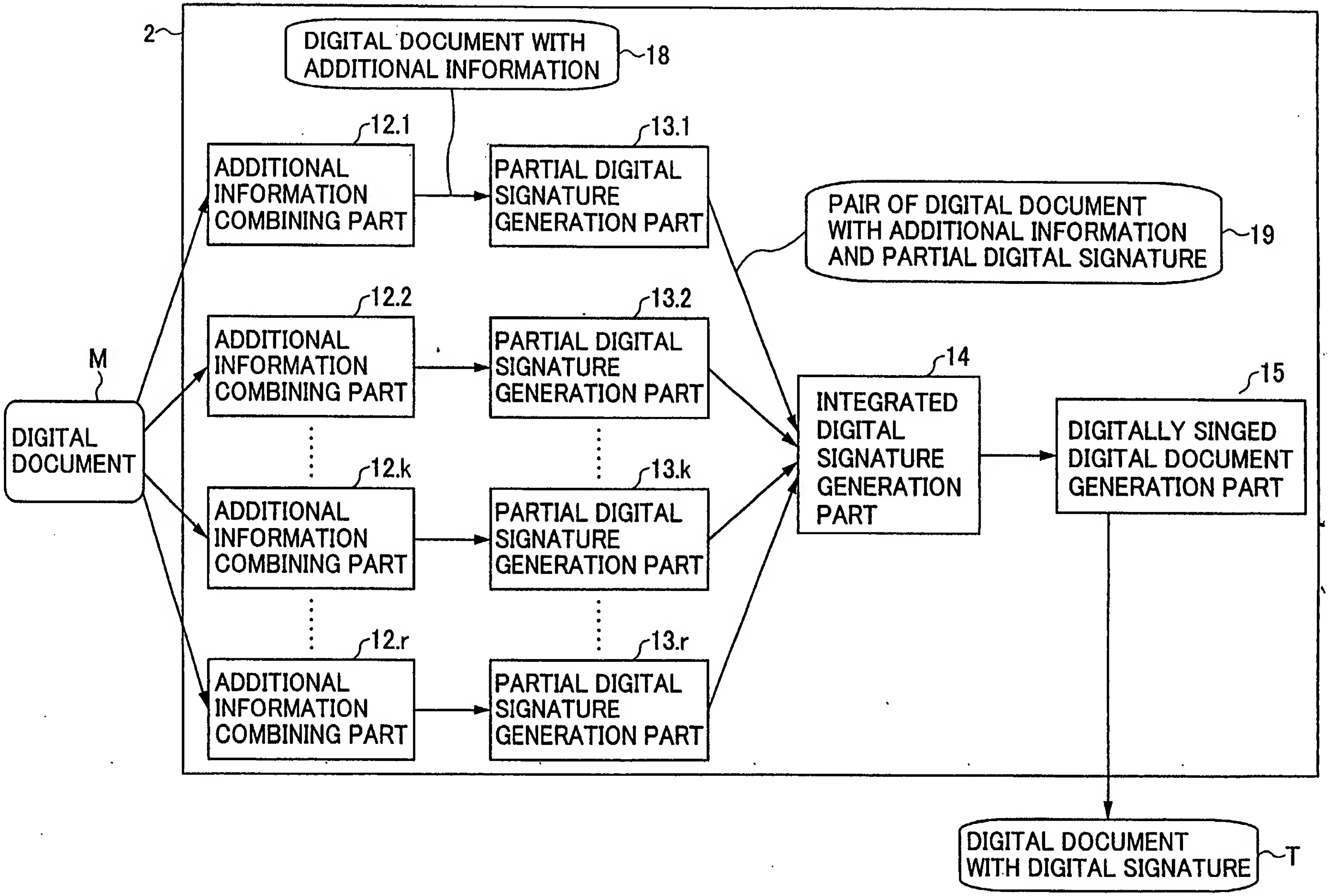

2
DIGITAL DOCUMENT WITH ADDITIONAL INFORMATION
18
M
DIGITAL DOCUMENT
12.1
ADDITIONAL INFORMATION COMBINING PART
12.2
ADDITIONAL INFORMATION COMBINING PART
12.k
ADDITIONAL INFORMATION COMBINING PART
12.r
ADDITIONAL INFORMATION COMBINING PART
13.1
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.2
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.k
PARTIAL DIGITAL SIGNATURE GENERATION PART
13.r
PARTIAL DIGITAL SIGNATURE GENERATION PART
PAIR OF DIGITAL DOCUMENT WITH ADDITIONAL INFORMATION AND PARTIAL DIGITAL SIGNATURE
19
14
INTEGRATED DIGITAL SIGNATURE GENERATION PART
15
DIGITALLY SINGED DIGITAL DOCUMENT GENERATION PART
DIGITAL DOCUMENT WITH DIGITAL SIGNATURE
T

FIG.12

k	r	A	B	B/A
3	5	6.5	30.9	4.75
4	7	15.0	83.0	5.53
5	9	26.5	165	6.23
6	11	44.4	280	6.31
7	13	68.9	430	6.24
8	15	92.4	617	6.68
9	17	127.9	842	6.59
10	19	171.4	1110	6.47

FIG.13

k	r	A	B	C	D	D/B
3	5	60.8	304.0	6,144	30,720	85
4	7	75.1	525.7	6,144	43,008	72
5	9	94.4	849.6	6,144	55,296	59
6	11	123.6	1359.6	6,144	67,584	46
7	13	163.3	2122.9	6,144	79,872	35
8	15	200.3	3004.5	6,144	92,160	29
9	17	256.7	4363.9	6,144	104,448	23
10	19	325.4	6182.6	6,144	116,736	18

FIG.14

k	r	A	B	C	D	D/B
3	5	60.8	382.0	12,288	61,440	161
4	7	75.1	629.7	12,288	86,016	137
5	9	94.4	979.6	12,288	110,592	113
6	11	123.6	1515.6	12,288	135,168	89
7	13	163.3	2304.9	12,288	159,744	69
8	15	200.3	3212.5	12,288	184,320	57
9	17	256.7	4597.9	12,288	208,896	45
10	19	325.4	6442.6	12,288	233,472	36